WHAT IS CLAIMED IS:

1. A method of controlling information flow through a firewall, said method comprising:

determining an incoming packet community set (PCS) of a first data packet received on an interface of said firewall;

discarding said first data packet in response to detecting said PCS is not a subset of an interface community set (IFCS) of said interface; and

processing said first data packet in response to detecting said PCS is a subset of said IFCS.

2. The method of claim 1, wherein said determining comprises determining a source network address community set (NACS) of said first data packet.

3. The method of claim 1, wherein said determining comprises determining a source network service community set (NSCS) of said first data packet.

4. The method of claim 1, wherein said incoming PCS is encoded in a header of said first data packet, and wherein said determining comprises decoding said incoming PCS from said header of said first data packet.

5. The method of claim 1, wherein said processing comprises matching said first data packet to a first rule of a plurality of rules of said firewall.

6. The method of claim 5, wherein said first rule includes a PCS attribute, and wherein said processing further comprises performing a first action in response to detecting said PCS of said first data packet does not match said PCS attribute, and wherein said

processing further comprises performing a second action in response to detecting said PCS of said first data packet matches said PCS attribute.

7. The method of claim 6, wherein said first action comprises discarding said first data packet.

8. The method of claim 6, wherein said second action comprises changing said PCS to a second PCS in response to detecting said first rule includes forwarding said first data packet, wherein said second PCS is indicated by said first rule.

9. The method of claim 8, further comprising:

comparing said second PCS with a destination community set of said first data packet;

discarding said first data packet in response to detecting said second PCS is not a subset of said destination community set; and

processing said first data packet in response to detecting said second PCS is a subset of said destination community set.

10. The method of claim 9, wherein said destination community set is a network address community set (NACS).

11. The method of claim 9, wherein said destination community set is a network service community set (NSCS).

12. The method of claim 9, wherein said processing comprises:

transmitting said first data packet via an output interface of said firewall in response to detecting said second PCS is a subset of the interface community set (IFCS) of said output interface; and

discarding said first data packet in response to detecting said second PCS is not a subset of said IFCS.

13. The method of claim 12, wherein said processing further comprises encoding said second PCS in a header of said first data packet.

14. The method of claim 13, further comprising recording an event corresponding to said first data packet in response to detecting said outgoing PCS is not a subset of said destination community set.

15. The method of claim 1, further comprising consulting a community information base (CIB).

16. The method of claim 15, wherein said CIB includes community set information corresponding to network addresses, network services, and interfaces.

17. The method of claim 12, further comprising recording an event corresponding to said first data packet in response to detecting said first data packet is discarded.

18. A node configured to act as a firewall, wherein said node comprises:

a processing unit, wherein said processing unit is configured to determine an incoming packet community set (PCS) of a first data packet received on an interface of said node, discard said first data packet in response to detecting said PCS is not a subset of an interface community set (IFCS) of

said interface, and process said first data packet in response to detecting said PCS is a subset of said IFCS; and

a community information base coupled to said processing unit.

19. The node of claim 18, wherein said processing unit is configured to determine said incoming PCS by determining a source network address community set (NACS) of said first data packet.

20. The node of claim 18, wherein said processing unit is configured to determine said incoming PCS by determining a source network service community set (NSCS) of said first data packet.

21. The node of claim 18, wherein said incoming PCS is encoded in a header of said first data packet, and wherein said processing unit is configured to determine said incoming PCS by decoding said incoming PCS from said header of said first data packet.

22. The node of claim 18, wherein said processing unit is configured to process said first data packet by matching said first data packet to a first rule of a plurality of rules of said firewall.

23. The node of claim 22, wherein said first rule includes a PCS attribute, and wherein said processing unit is further configured to process said data packet by performing a first action in response to detecting said PCS of said first data packet does not match said PCS attribute, and wherein said processing unit is further configured to process said data packet by performing a second action in response to detecting said PCS of said first data packet matches said PCS attribute.

24. The node of claim 23, wherein said first action comprises discarding said first data packet.

25. The node of claim 23, wherein said second action comprises changing said PCS to a second PCS in response to detecting said first rule includes forwarding said first data packet, wherein said second PCS is indicated by said first rule.

26. The node of claim 25, wherein said processing unit is further configured to:

compare said second PCS with a destination community set of said first data packet;

discard said first data packet in response to detecting said second PCS is not a subset of said destination community set; and

process said first data packet for output in response to detecting said second PCS is a subset of said destination community set.

27. The node of claim 26, wherein said destination community set is a network address community set (NACS).

28. The node of claim 26, wherein said destination community set is a network service community set (NSCS).

29. The node of claim 26, wherein said processing said first data packet for output comprises:

transmitting said first data packet via an output interface of said firewall in response to detecting said second PCS is a subset of the interface community set (IFCS) of said output interface; and

discarding said first data packet in response to detecting said second PCS is not a subset of said IFCS.

30. The node of claim 29, wherein said processing unit is further configured to encode said second PCS in a header of said first data packet prior to said transmitting.

31. The node of claim 30, wherein said processing unit is further configured to record an event corresponding to said first data packet in response to detecting said outgoing PCS is not a subset of said destination community set.

32. The node of claim 18, wherein said processing unit is configured to consult said community information base (CIB).

33. The node of claim 32, wherein said CIB includes community set information corresponding to network addresses, network services, and interfaces.

34. The node of claim 29, further comprising recording an event corresponding to said first data packet in response to detecting said first data packet is discarded.

35. A computer network comprising:

a node configured to act as a firewall, wherein said node comprises:

a processing unit, wherein said processing unit is configured to determine an incoming packet community set (PCS) of a first data packet received on an interface of said node, discard said first data packet in response to detecting said PCS is not a subset of an interface community set (IFCS) of said interface, and process said first data packet in response to detecting said PCS is a subset of said IFCS; and

a community information base coupled to said processing unit;

a first computer network coupled to said node; and

a second computer network coupled to said node.

36. The computer network of claim 35, wherein said node is configured to determine said incoming PCS by determining a source network address community set (NACS) of said first data packet.

37. The computer network of claim 35, wherein said node is configured to determine said incoming PCS by determining a source network service community set (NSCS) of said first data packet.

38. The computer network of claim 35, wherein said incoming PCS is encoded in a header of said first data packet, and wherein said node is configured to determine said incoming PCS by decoding said incoming PCS from said header of said first data packet.

39. The computer network of claim 35, wherein said node is configured to process said first data packet by matching said first data packet to a first rule of a plurality of rules of said firewall.

40. The computer network of claim 39, wherein said first rule includes a PCS attribute, and wherein said node is further configured to process said data packet by performing a first action in response to detecting said PCS of said first data packet does not match said PCS attribute, and wherein said node is further configured to process said data packet by performing a second action in response to detecting said PCS of said first data packet matches said PCS attribute.

41. The computer network of claim 40, wherein said first action comprises discarding said first data packet.

42. The computer network of claim 40, wherein said second action comprises changing said PCS to a second PCS in response to detecting said first rule includes forwarding said first data packet, wherein said second PCS is indicated by said first rule.

43. The computer network of claim 42, wherein said node is further configured to:

compare said second PCS with a destination community set of said first data packet;

discard said first data packet in response to detecting said second PCS is not a subset of said destination community set; and

process said first data packet for output in response to detecting said second PCS is a subset of said destination community set.

44. The computer network of claim 43, wherein said destination community set is a network address community set (NACS).

45. The computer network of claim 43, wherein said destination community set is a network service community set (NSCS).

46. The computer network of claim 43, wherein said processing said first data packet for output comprises:

transmitting said first data packet via an output interface of said firewall in response to detecting said second PCS is a subset of the interface community set (IFCS) of said output interface; and

discarding said first data packet in response to detecting said second PCS is not a subset of said IFCS.

47. The computer network of claim 46, wherein said node is further configured to encode said second PCS in a header of said first data packet prior to said transmitting.

48. The computer network of claim 47, wherein said node is further configured to record an event corresponding to said first data packet in response to detecting said outgoing PCS is not a subset of said destination community set.

49. The computer network of claim 35, wherein said node is configured to consult said community information base (CIB).

50. The computer network of claim 49, wherein said CIB includes community set information corresponding to network addresses, network services, and interfaces.

51. The computer network of claim 46, further comprising recording an event corresponding to said first data packet in response to detecting said first data packet is discarded.